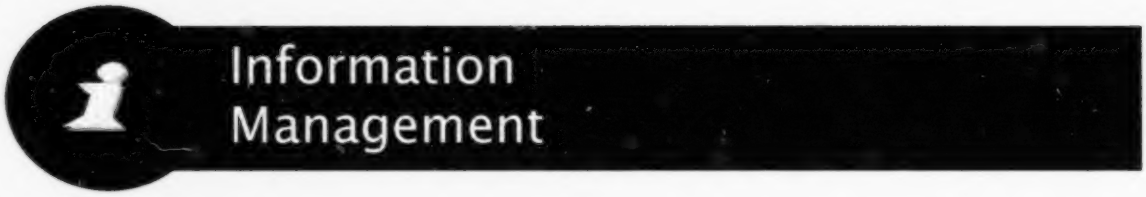

Managing Personal Digital Assistants (PDAs)

December 2005

Alberta
Government

Produced by:

Information Management Branch
Government and Program Support Services Division
Alberta Government Services
3rd Floor, Commerce Place
10155 – 102 Street
Edmonton, Alberta, Canada
T5J 4L4

Office Phone: (780) 422-2657
Fax: (780) 427-1120

Web Site:
www.im.gov.ab.ca

©Government of Alberta

ISBN 0-7785-3687-4

106-01950/

Contents

1. Introduction 1
Scope 1
Purpose 1

2. Government of Alberta Policies Related to PDAs 2
Authorized use of Government of Alberta systems 2
Acceptable use of Internet and e-mail 3
Transmission of personal information 3
Managing messages as records 4

3. Establishing Ministry Standards and Guidelines for PDA Use 5
Appropriate use of PDAs 5
Integrating the management of PDA messages with records management systems 6
Security 7
Complying with FOIP 8
Monitoring of PDA messages 9
Usage practices 9

Appendix 1: Model Policy and Guidelines for PDAs 10
Policy 10
Guidelines 12

1. Introduction

Personal Digital Assistants (PDAs) such as Blackberries®, Palm Trēos™, and the Motorola Q have become important tools in today's business environment. They support a mobile workforce by enabling a range of communications, document sharing, and web functions at any time, and with complete mobility of the user.

These devices typically combine the capability of a cell phone with other communication activities such as e-mail. They also enable the user to create and share files, send and receive text messages, and browse the web and use web-based services[1]. More recently, like cell phones, they often have the capability of taking, storing and sending photographs[2].

Like other business tools that create, store and transmit recorded information, users need to understand the appropriate use of PDAs in a business context.

Scope

This guide has been developed for information management professionals in the Government of Alberta. It is designed to help ministries establish standards and guidelines to help employees meet their responsibilities, including government recordkeeping requirements, and to use these business tools effectively.

[Ed. Note: This is an interim guide that focuses on issues related specifically to the use of PDAs. Because of the convergence of various technologies, this guide will, in the future, be integrated into a more comprehensive guide covering electronic mail, PDAs and other electronic messaging services.]

Purpose

The purpose of this guide is to:

- bring together existing policies and legislation that govern the management of information created or transmitted using PDAs; and
- identify guidelines and practices that should be established at the ministry level.

---

[1] Current bandwith available for transmission does not make it very practical to browse the web or use web-based services. However, as bandwidth increases these services become more practical from a PDA.

[2] While newer PDAs combine telephone capability and various Internet functions with other features that synchronize (e.g., calendar functions) with the desktop, earlier PDAs had only the capability to synchronize with the desktop. While much of the advice provided in this guide will be applicable to all PDAs, certain advice will depend on the features enabled on particular PDAs.

2.
Government of Alberta Policies Related to PDAs

Several Government of Alberta policies relate to the use and management of information created or transmitted on PDAs.

These policies relate to:

- the authorized use of the Government of Alberta systems;
- the acceptable use of Internet and e-mail;
- the handling of personal information; and
- government recordkeeping requirements.

It should be noted that none of these policies explicitly mentions PDAs. In some cases (e.g., acceptable use and government recordkeeping), the policies and legal requirements are broad enough to apply to PDAs. In other cases (e.g., the transmission of personal information), the policy can be inferred to apply to the use of PDAs because of its application to the technology used to transmit content from a PDA.

Authorized use of Government of Alberta systems

Access to Government of Alberta systems will be based on business needs and will normally be provided to all employees of the Government of Alberta.

The Government of Alberta Information Technology Security Policy allows access to government systems by staff of other organizations if there is a clear business need for the services, and the individuals are contracted by or acting as an agent for a ministry.

PDAs issued by a ministry are property of the Government of Alberta. Moreover, they interface with government systems. As such, PDAs would fall under the government policies related to acceptable use and security.

The Government of Alberta had adapted the Information Security Forum "Report on Securing PDA Devices: Best Practices." This guide can be found at: https://www.sharp.gov.ab.ca/secure/docDisplay.cfm?DocID=4254.

Acceptable use of Internet and e-mail

Most PDAs are enabled to browse the web and to send and receive e-mail. Thus, PDAs fall within the Use of Government of Alberta Internet and E-Mail. The policy describes the conditions of use by Alberta government employees of both the Internet and e-mail. Key components of this policy are:

- Authorized users of government systems are encouraged to use these systems and tools to fulfill their employment duties and to support their ministry's business goals.
- Personal use of systems is permitted, provided the use is consistent with professional conduct, does not detract from the performance of employment duties, and is not used for personal financial gain.
- Users must not bring disrepute to the Government of Alberta.
- Use of the network must not conflict with responsibilities outlined in the Official Oath of Office and the Code of Conduct and Ethics for the Public Service of Alberta.
- Users must not violate applicable laws and are expected to use discretion and good judgment when using systems.
- All users, including remote access users connecting to government systems through the Internet, must take reasonable precautions to safeguard government systems and not to cause damage to government systems.

Transmission of personal information

The Government of Alberta Policy for the Transmission of Personal Information via Electronic Mail and Facsimile was adopted by Deputy Ministers in September 2001 and later updated in July 2002 to include implementation guidelines for ministries.

Any PDA message will be using the public network for transmission (like electronic mail). Thus, this policy is also applicable to information transmitted from PDAs.

The policy states that any documentation or records containing personal information must not be transmitted by electronic mail or facsimile unless:

- personal identifiers have been removed;
- the message is encrypted in such a way that the message sender and recipient can both be authenticated; or
- other means are employed by both the sender and the recipient to ensure confidentiality is maintained.

Managing messages as records

In addition to these policies, various statutes and regulations affect the management of messages created and received on PDAs.

Messages created or compiled on, or sent or received on Government of Alberta systems are records of the government. These records:

- are the property of the Government of Alberta;
- must be managed according to the provisions of the Records Management Regulation and any records management policies, standards and procedures issued by the Alberta Records Management Committee (ARMC) and Alberta Government Services (the ministry responsible for the government's records management program);
- are bound by the *Historical Resources Act* which ensures the permanent preservation of government records of archival value so that they are available to Albertans in the future;
- are subject to both the access provisions and the protection of privacy provisions of the *Freedom of Information and Protection of Privacy Act*; and
- can contain personal health information and as such may be bound by the *Health Information Act* which governs the collection, use and disclosure of health information, how health information must be handled and protected, and the right of individuals to access their own health information in the custody or under control of custodians as defined under the Act, including the Ministry of Health and Wellness.

3.
Establishing Ministry Standards and Guidelines for PDA Use

Records generated and received on PDAs can be managed successfully through a combination of standards and guidelines, systems design and end-user training.

Ministries should establish clear standards and guidelines related to the use of PDAs. Typical guidelines and practices would relate to:

- appropriate use of PDAs;
- integrating the management of messages with other records management practices;
- protecting the security of messages and information stored on the PDA device;
- compliance with freedom of information and privacy requirements;
- the ministry's practices for monitoring and recording PDA messages; and
- effective usage practices for sending PDA messages, including roles and responsibilities for managing PDA-generated messages.

See the Sample Ministry Standards and Guidelines (Appendix 1) for an example of how such guidelines and practices can be brought together in a simple form.

Ministries should ensure the guidelines and practices are communicated to staff and that training is provided where needed.

Appropriate use of PDAs

Because of the wide variety of uses of PDAs, employees will need to be informed of acceptable and unacceptable use of PDAs within the Government of Alberta.

First, employees should understand the impact of the policy on the Use of Government of Alberta Internet and E-mail. This would include the taking and storage of photographs as well as the content of messages composed on PDAs.

If ministry-issued PDAs have web capability, then employees should understand the ministry's policy on the use of instant messaging on systems outside of the government network.

Finally, employees should not use their own, non-government PDA for the conduct of government business.

Integrating the management of PDA messages with records management systems

The management of PDA messages needs to be integrated with other records in the custody or under the control of each ministry.

Synchronization of e-mail messages

Employees should be encouraged to regularly synchronize their PDAs with the ministry's e-mail application. In this way, messages can be managed in the same way as other e-mail records are managed.

Text messages

Text messages are not captured during synchronization of PDAs with the desktop. As such, they would not be captured into the ministry's recordkeeping system. Employees should be informed not to use text messaging to convey decisions, approvals, directions and other substantive business.

Files

Many PDAs enable the user to create a file in an application or download a file from the corporate network or Internet. Files created on a PDA or downloaded onto a PDA are not captured through a synchronization process. Thus, users must ensure that any file created on a PDA that is a record of government business (i.e., an official record) is captured in the ministry's recordkeeping system. The easiest way to achieve this is, if a file is created, users can e-mail the file to themselves so that it can be captured in the ministry's recordkeeping system.

Deleting e-mail messages

While most e-mail messages will be deleted during synchronization, several types of messages often continue to reside on the PDA. These may include:

- messages from Listservs™ (both external and SHARP-hosted);
- calendar and meeting notices that you have responded to from your desktop e-mail application;
- text messages; and
- messages you reply to.

These messages should be deleted regularly as transitory records.

Security

Information technology systems, including the use of PDAs, must conform to the Government of Alberta Information Technology Security Policy.

One of the most significant security threats involves the loss of the PDA. Since PDA devices are small, many people have left them behind at meetings, in a restaurant or in automobiles. Users should keep track of their PDA at all times while outside the office. Also, it is a good practice to set up passwords to enable use of the PDA. In this way, if the PDA is lost, information stored on it is less likely to be accessible to unauthorized users.

Like electronic mail, there are several additional security risks associated with using PDAs to conduct business. These risks include:

- the simple misdirection of messages to unintended recipients;
- the non-delivery of messages; or
- redirection of government records to non-government mail systems (for example, home computers or other public access systems).

Ministries should take all appropriate physical and technical security measures to protect the information transmitted to and from or contained on PDAs.

Practices and guidelines should help users understand the nature of security related to PDAs. These may include a description of:

- **Viruses:** To date, there have been few known PDA viruses. However, this may change as PDAs become more ubiquitous in the workplace. In addition, the PDA may act as a conduit for malicious code, or viruses to spread between PCs during the synchronization process. PCs used for synchronization should be scanned regularly for viruses. (Note: Virus protection on the PC is likely sufficient to catch and protect against any PDA resident virus).
- **Personal Identification Numbers (PINs)**: Some PDAs, such as Blackberries®, have unique identifiers called a PIN. Knowing the personal identifier of someone's PDA allows the sending of text messages outside the e-mail system from one PDA to another PDA. As these messages are not captured during the synchronization process, these messages would not be captured into the ministry's recordkeeping system. Ministries should only enable PIN capability where there is a clear business need for it. If PIN-to-PIN capability is activated, users should be instructed on the appropriate use of PIN-to-PIN messaging (i.e., not to conduct ministry business via PIN-to-PIN messaging) to ensure compliance with legislation and Government of Alberta policies).

- **Security Labels**: Protocols for the use of security classification labels such as "confidential," should be explained to users. Such labels can be attached to e-mail messages by senders to alert recipients about special privacy or security handling requirements. The guidelines should describe the circumstances where these measures may be employed and the practices to be used in particular circumstances.
- **System and Audit Trails**: System audit trails automatically record the creation, transmission and receipt, filing and retrieval, updates, and deletion of messages sent on a PDA, including PIN-to-PIN messaging. Users should be informed about them.
- **Encryption**: Users should be made aware of what encryption methods are available to them, and the practices for using encryption. If encryption methods are available, appropriate safeguards to recover encrypted messages must be in place.

More information on securing PDA devices can be found in the Government of Alberta's "Report on Securing PDA Devices: Best Practices" at https://www.sharp.gov.ab.ca/secure/docDisplay.cfm?DocID=4254.

Complying with FOIP

Any records retained on PDAs are in the custody or under the control of the ministry and, thus, may be responsive to a request for information under the *Freedom of Information and Protection of Privacy Act* (FOIP).

The same rules apply to records retained on PDAs as to other types of information subject to a request. No information that may be responsive to a FOIP request may be deleted after the request has been received until the request has been completed and all applicable review periods have expired. This remains the case even where approved records retention and disposition schedules are in place.

In addition, the government's Policy for the Transmission of Personal Information via Electronic Mail and Facsimile prohibits the transmission of personal information via electronic mail unless:

- personal identifiers have been removed, or
- the message is encrypted in such a way that the message sender and recipient can both be authenticated, or
- other means are used by both the sender and recipient to ensure confidentiality and protection of privacy is maintained.

The same policy would apply to files or messaged transmitted from a PDA.

Monitoring of PDA messages

Systems are routinely monitored for capacity and storage to maintain the efficiency of the system. However, the ministry's guidelines should clearly state under what conditions the system administrator and other authorized individuals will monitor an individual's PDA messages. These conditions should take into account the following factors:

- users of the system may have an expectation of privacy;
- general monitoring of e-mail communications for unspecified purposes should not be allowed;
- there will be no secret monitoring or search, except as permitted by law enforcement measures; and
- all collection, use and disclosure of personal information involving an e-mail system will be done in accordance with the legal requirements of the *Freedom of Information and Protection of Privacy Act*.

In addition to messages that are captured in the ministry's system, users should be reminded that the PDA and all information stored on the PDA is government property. In rare instances, the ministry may need to recall the PDA to access information that is stored on the PDA.

Usage practices

Ministries should also establish common usage practices that support the effective and efficient use of PDAs. The usage practices will vary depending on the nature of the business and the organization, but could include the following:

- Establish who is responsible for managing the PDA record. This is especially important in work groups or in other instances where many people might receive the same message. Records should be managed as they relate to business activities of the ministry (i.e., the office of primary responsibility should be charged with managing official government records created, received or retained on PDAs. This can avoid duplication of effort.)
- Ensure that when dealing with sensitive information, the message is sent to the correct recipient(s). This is particularly important if the message is being sent to a long distribution list. Some common practices related to this issue include:
  - ensure they have the correct e-mail address of recipients;
  - verify that a distribution list is up-to-date and that the recipients for a particular message are authorized to receive the message before sending it to the entire list; and
  - do not forward another author's e-mail message to a discussion group, Listserv™, newsgroup or post it on an electronic bulletin board without the author's permission.

Appendix 1: Model Policy and Guidelines for PDAs

This section contains an example of ministry policy related to the use of PDAs. Based on their business needs, ministries may want to implement alternate (or additional) policy statements and guidelines.

Policy

Scope

This policy applies to all employees using PDAs. When conducting government business, employees should only use PDAs that have been issued by [insert ministry name].

Related policies

As PDAs enable users to a wide range of applications, employees should refer to [insert ministry name] policies and guidelines on e-mail and instant messaging.

Authorized services

- Users will only use [insert ministry name] authorized services. Text messaging and instant messaging should NOT be used to convey decisions, approvals, directions, and other substantive or official business.
- PIN-to-PIN messaging will only be enabled where there is a clear business need.

Acceptable use

- Employees will not use their personal (non-government) PDA for the conduct of government business. Personal PDAs will not be linked into the ministry network.
- Users will use [insert ministry name]-issued PDAs to fulfill their employment duties and to support the ministry's business goals.
- Personal use of your PDA is acceptable, provided the use is consistent with professional conduct, does not detract from the performance of employment duties, and is not used for personal financial gain.
- Users must not bring disrepute to the Government of Alberta.
- Use of the PDA must not conflict with responsibilities outlined in the Official Oath of Office and the Code of Conduct and Ethics for the Public Service of Alberta.
- Users must not violate applicable laws and are expected to use discretion and good judgment.

- All users, including remote access users connecting to government systems through the Internet, must take reasonable precautions to safeguard government systems and not to cause damage to government systems.
- [insert ministry/branch name] may initiate investigations of PDA usage as warranted.

Recordkeeping requirements

Any information created or compiled on, or sent or received on Government of Alberta systems are records of the government. These records:

- are the property of the Government of Alberta;
- must be managed according to the provisions of the Records Management Regulation and [insert ministry name] records management policies, standards and procedures.

All files and e-mail that are official records must be captured in the [insert ministry name] records management system and managed throughout their life cycle.

Security

- Users will keep the PDA with them or in a secure location at all times.
- Users will report any loss of a PDA or damage to a PDA immediately to [insert name/position].
- All users will establish a "power-on" password to enable access to operation their PDA and to prevent unauthorized users from accessing their PDA.

Roles and responsibilities

Messages sent to, or received by, and retained on a PDA are in the custody and control of the ministry. Therefore, messages are subject to the access and privacy rules of the *Freedom of Information and Protection of Privacy Act* and must be managed according to the Records Management Regulation. Individual users are responsible for managing files and messages according to the rules set out in legislation, Government of Alberta and ministry policies and related procedures.

Review process

This policy will be reviewed yearly or earlier, if necessary. The policy has been approved by [insert position title].

Guidelines[3]

Synchronizing e-mail

Users should synchronize e-mail (including calendar and task functions) regularly. Once synchronization has occurred, users should delete any unnecessary messages that have not been deleted during the synchronization process.

Style

Users will employ a style of writing that is business-like.

Forwarding messages

Users will not forward sensitive business-related messages to non-secure, non-government e-mail systems (e.g., Hotmail accounts) or PDAs.

Managing official records

Users will file instant messages that qualify as official records in the electronic information management system. [insert ministry procedure]

Users will delete unneeded transitory records from a PDA on a regular basis.

Privacy

Messages containing personal information must not be transmitted using a PDA unless:

- personal identifiers have been removed;
- the message is encrypted in such a way that the message sender and recipient can both be authenticated; or
- other means are employed by both the sender and the recipient to ensure confidentiality is maintained.

[Insert recommended ministry procedure.]

FOIP and litigation

If the ministry receives a Freedom of Information and Protection of Privacy (FOIP) request or becomes involved in litigation, employees must not delete any content that is responsive to the request that is contained on their PDA until advised by the FOIP coordinator or the ministry's solicitor that the request or the legal action is complete.

---

[3] These guidelines are examples of areas where employees will need guidance. Each will need to be accompanied by procedures the ministry will use in its particular records, systems and information management environment.